



CVE-2017-7781

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-7781
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-11 21:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An error occurs in the elliptic curve point addition algorithm that uses mixed Jacobian-affine coordinates where it can yield a

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All

References

Reference
Mozilla Firefox CVE-2017-7781 Man in the Middle Security Bypass Vulnerability
Mozilla Firefox Multiple Bugs Let Remote Users Spoof Content, Obtain Potentially Sensitive Information, Deny Service and Execute Arbitrary C
1352039 - (CVE-2017-7781) Issue with elliptic curve addition in mixed Jacobian-affine coordinates
Security vulnerabilities fixed in Firefox 55 — Mozilla
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)